CLAIMS

1. A method of preventing theft of an organization property, comprising:
   a. generating an authentication result from comparing stored identification information with collected identification information of the organization property; and
   b. transmitting a plurality types of network packets containing the authentication result to a plurality of organization servers via a network.
2. The method according to claim 1, 1(a) further comprises:
   retrieving the stored identification information and network addresses of the organization servers from a tamper-resistant storage location.
3. The method according to claim 2, 1(b) further comprises:
   assembling the plurality types of network packets with the network addresses and information indicative of a current location of the organization property.
4. The method according to claim 3, further comprises:
   a. assembling and transmitting an intranet network packet to an intranet server; and
   b. in response to non-acknowledgement from the intranet server, assembling and transmitting an internet network packet to an internet server.
5. The method according to claim 2, further comprises:

retrieving the collected identification information from the organization property.

6. The method according to claim 2, further comprises:

retrieving the collected identification information from an electronic system that contains the organization property.

7. The method according to claim 5, the collected identification information comprises an Internet Protocol address assigned to the organization property.

8. The method according to claim 6, the collected identification information comprises device identification information of the electronic system.

9. A machine readable medium having embodied thereon instructions, which when executed by a machine, causes the machine to prevent theft of an organization property, the instructions comprising:

   a. generating a authentication result from comparing stored identification information with collected identification information of the organization property; and

   b. transmitting a plurality of network packets that are indicative of the authentication result to a plurality of organization servers via a network.

10. The machine readable medium according to claim 9, the instructions for 9(a) further comprises:

retrieving the stored identification information and network addresses of the organization servers from a tamper-resistant storage location.

11. The machine readable medium according to claim 10, the instructions for 9(b) further comprises:

assembling the plurality types of network packets with the network addresses and information indicative of a current location of the organization property.

12. The machine readable medium according to claim 11, the instructions further including:

a. assembling and transmitting an intranet network packet to an intranet server; and

b. in response to non-acknowledgement from the intranet server, assembling and transmitting an internet network packet to an internet server.

13. The machine readable medium according to claim 10, the instructions further including:

retrieving the collected identification information from the organization property.

14. The machine readable medium according to claim 10, the instructions further including:

retrieving the collected identification information from an electronic system that contains the organization property.

15. The machine readable medium according to claim 13, the collected identification information comprises an Internet Protocol address assigned to the organization property.

16. The machine readable medium according to claim 14, the collected identification information comprises device identification information of the electronic system.

17. A theft prevention system for detecting theft of an organization property, comprising:

a. a plurality of organization servers coupled to a network;

b. a tamper-resistant storage location to maintain stored identification information of the organization property and network addresses of the organization servers;

c. a theft monitor, coupled to the tamper-resistant storage location, to generate a authentication result by comparing stored identification information with collected identification information of the organization property; and

d. a network access controller, coupled to the theft monitor, to transmit a plurality types of network packets containing the authentication result to the organization servers via the network.

18. The theft prevention system according to claim 17, the theft monitor further assembles the plurality types of network packets with the network addresses and information indicative of a current location of the organization property.

19. The theft prevention system according to claim 18, the theft monitor further:

a. transmits an intranet network packet to an intranet server; and

b. in response to non-acknowledgement from the intranet server, transmits an internet network packet to an internet server.

20. The theft prevention system according to claim 18, the theft monitor further:

a. causes the network access controller to transmit an intranet network packet to an intranet server; and

b. in response to non-acknowledgement from the intranet server, causes the network access controller to transmit an internet network packet to an internet server.

21. The theft prevention system according to claim 17, the theft monitor further retrieves the collected identification information from the organization property.

22. The theft prevention system according to claim 17, the theft monitor further retrieves the collected identification information from an electronic system that contains the organization property.

23. The theft prevention system according to claim 21, the collected identification information comprises an Internet Protocol address assigned to the organization property.

24. The theft prevention system to claim 22, the collected identification information comprises device identification information of the electronic system.